ABSTRACT OF THE DISCLOSURE

A modular arithmetic apparatus has a plurality of base parameter sets in read only memories. A base selection unit in the modular arithmetic apparatus selects one of the base parameters sets according to an input modulus p. A plurality of operation units 30, in the modular arithmetic apparatus, perform an arithmetic operation according to the selected base parameter set in parallel and obtain an arithmetic result.